EXHIBIT 2

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/597,486	11/22/2006	Jen-Wei Kuo	KUO 15 JUN05	6774

7590   08/08/2014

Kuo Jen Wei
7005 Wilderness Road
Raliegh, NC 27613

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
08/08/2014	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD
_____

Ex parte JEN-WEI KUO
_____

Appeal 2012-002260
Application 11/597,486
Technology Center 2400
_____

Before ROBERT E. NAPPI, BRUCE R. WINSOR,
and MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's
Final Rejection of claims 1–3, 5, 7–9, 14, 18, 21–24, 27, 28, 33, 34, 36, 39,
45, 48, 65–69, 72–74, 90–92, 95, 98, 100, 102–104, 106–112, and 114–116,
which constitute all the claims pending in this application. Claims 4, 6,
10–13, 15–17, 19, 20, 25, 26, 29–32, 35, 37, 38, 40–44, 46, 47, 49–64, 70,
71, 75–89, 93, 94, 96, 97, 99, 101, 105, 113, and 117 have been cancelled.
We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Appeal 2012-002260
Application 11/597,486

STATEMENT OF THE CASE

Introduction

Appellant's invention relates to a security management system and method for protecting endpoint computing systems within a network. (*See* Spec. 1:4-6.) Exemplary independent claim 1 reads as follows:

> 1. An apparatus associated with an endpoint and configurable between a network and a host of the endpoint,
> comprising computational resources, the computational resources at least comprising one processor, wherein
> the computational resources are not accessible by the host, are accessible over a secure connection by a management server, and are configured to provide an open platform able to execute security function software modules from multiple vendors and provide immunization and defense functionality to protect the host.

Rejection

Claims 1–3, 5, 7–9, 14, 18, 21–24, 27, 28, 33, 34, 36, 39, 45, 48, 65–69, 72–74, 90–92, 95, 98, 100, 102–104, 106–112, and 114–116 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Lynn et al. (US 7,058,796 B2, issued June 6, 2006) (hereinafter "Lynn"). (*See* Ans. 4–17.)

ANALYSIS

1. *Claims 1–3, 5, 7–9, 14, 18, 21–24, 27, 28, 33, 34, 36, 39, 45, 48, 65–69, 72–74, 95, 98, 100, 102–104*

Appellant argues that the Examiner has erred in rejecting independent claim 1 because Lynn fails to disclose, *inter alia*, computational resources that (1) are not accessible by a host of an endpoint; (2) execute multiple

Appeal 2012-002260
Application 11/597,486

security function software modules; and (3) provide immunization functionality. (*See* App. Br. 11, 13–15.) Independent claims 7, 18, 22, 27, 33, 48, 65, and 95 recite features similar to at least one of these three features. (*See id.* at 24–29.) We agree with Appellant.

Further, we note that the issue of whether Lynn discloses the three features is dispositive, and we therefore need not address Appellant's other arguments with respect to claim 1.

> *a.   Computational resources that are not accessible by a host of an endpoint*

In rejecting claim 1, the Examiner cites a passage in Lynn that describes various hardware components as disclosing the feature computational resources that are not accessible by a host of an endpoint. (*See* Ans. 4–5; *see also* Lynn, col. 8, l. 44–col. 9, l. 3.) Independent claims 18 and 48 recite similar features. As Appellant contends, the Examiner does not explain how the cited passage relates to any portion of the claimed feature. (*See* App. Br. 13.) In response, the Examiner takes the position that Lynn's system data store (SDS) corresponds to the recited computational resources and that Lynn's mobile computer system (e.g., device 210A) corresponds to the recited endpoint. (*See* Ans. 17.) The Examiner then cites another passage in Lynn, noting the SDS may be segregated physically within a single device and its storage elements may be located centrally. (*See* Ans. at 18; *see also* Lynn, col. 10, ll. 17–29.) In citing this passage, however, the Examiner does not identify any teaching that the SDS is not accessible by a host of the mobile computer system. Without any guidance from the Examiner on how to map the claimed feature to Lynn's teachings,

3

Appeal 2012-002260
Application 11/597,486

we are persuaded of error in the Examiner's finding that Lynn discloses computational resources that are not accessible by a host of an endpoint.

      b.   *Computational resources that execute multiple security function software modules*

In rejecting claim 1, the Examiner cites a passage in Lynn that describes various embodiments of the SDS as disclosing the feature computational resources that execute multiple security function software modules. (*See* Ans. 5; *see also* Lynn, col. 10, ll. 17–29.) Independent claims 7, 27, 33, 65, and 95 recite similar features. The Examiner points out that the cited passage discusses multiple independent data stores, (*see* Ans. 5, 19), which Lynn teaches may collectively comprise the SDS, (*see* Lynn, col. 10, ll. 23–26). As discussed above, the Examiner equates the SDS with computational resources. (*See* Ans. 17.) Accordingly, we understand the Examiner is equating the data stores with computational resources. As Appellant contends, however, the data stores alone do not constitute additionally executing multiple security function software modules. (*See* App. Br. 14.) Moreover, the Examiner does not identify in Lynn any teaching of a software module at all. (*See* Ans. 5, 19.) We are therefore persuaded of error in the Examiner's finding that Lynn discloses computational resources that execute multiple security function software modules.

      c.   *Computational resources that provide immunization functionality*

In rejecting claim 1, the Examiner cites a passage in Lynn that describes active defense mechanisms as disclosing the feature computational resources that provide immunization functionality. (*See* Ans. 5; *see also* Lynn, col. 28, ll. 33–41.) Independent claims 7, 18, 22, 33, and 48 recite

Appeal 2012-002260
Application 11/597,486

similar features. Drawing a distinction between defense and immunization functions, Appellant contends that the cited passage discusses only defense functions and fails to teach immunization functions. (*See* App. Br. 15.) In response, the Examiner cites another passage in Lynn that discusses monitoring wireless traffic over a wireless network. (*See* Ans. 19.) Without any explanation from the Examiner on how the additional passage teaches an immunization function, we are persuaded of error in the Examiner's finding that Lynn discloses computational resources that provide immunization functionality.

In view of the foregoing, we do not sustain the Examiner's § 102 rejection of claims 1–3, 5, 7–9, 14, 18, 21–24, 27, 28, 33, 34, 36, 39, 45, 48, 65–69, 72–74, 95, 98, 100, 102–104.

2.   *Claims 90–92*

Appellant argues that the Examiner has erred in rejecting independent claim 90 because Lynn fails to disclose, *inter alia*, a server that manages a security subsystem so as to eliminate direct access by vendor security management systems. (*See* App. Br. 20–21.) We agree with Appellant.

In rejecting claim 90, the Examiner cites a passage in Lynn that describes various embodiments of the SDS as disclosing the recited server. (*See* Ans. 13; *see also* Lynn, col. 10, ll. 17–29.) The Examiner points out that Lynn teaches multiple independent data stores. (*See* Ans. 13, 22.) Appellant contends, however, mere data stores do not constitute a server that manages a security subsystem so as to eliminate access by vendor security management systems. (*See* App. Br. 20.) In response, the Examiner additionally points out that Lynn teaches the SDS may be located centrally

Appeal 2012-002260
Application 11/597,486

or distributed across various locations. (*See* Ans. 22.) Without further discussion from the Examiner of how Lynn's teachings relate to the claimed feature, we are persuaded of error in the Examiner's finding that Lynn discloses a server that manages a security subsystem so as to eliminate direct access by vendor security management systems.

As the issue of whether Lynn discloses the recited server is dispositive, we need not address Appellant's other arguments with respect to claim 90. Accordingly, we do not sustain the Examiner's § 102 rejection of claims 90–92.

3.   *Claims 106–112 and 114–116*

Appellant states that claims 106–112 and 114–116 depend from claim 95. (*See* App. Br. 21.) We note, however, claim 106 is an independent claim with depending claims 107–112 and 114–116. None of Appellant's arguments with respect to claims 1 or 95 seems to apply to claim 106. Thus, Appellants have not identified an error in the Examiner's rejection of claims 106–112 and 114–116. We accordingly sustain the Examiner's §102 rejection of these claims.

DECISION

The Examiner's decision rejecting claims 106–112 and 114–116 is affirmed.

The Examiner's decision rejecting claims 1–3, 5, 7–9, 14, 18, 21–24, 27, 28, 33, 34, 36, 39, 45, 48, 65–69, 72–74, 90–92, 95, 98, 100, and 102–104 is reversed.

Appeal 2012-002260
Application 11/597,486

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv)(2011).

AFFRIMED-IN-PART

dw

Appeal 2012-002260

7